PIMA-01028-US

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　６月１１日

出願番号
Application Number: 特願２００１－１７５８７４

出願人
Applicant(s): 池田　実

２００１年　８月２４日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０７６２２３

【書類名】　特許願
【整理番号】　PIMA-13167
【提出日】　平成13年 6月11日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　千葉県船橋市習志野台２－２１－４
　【氏名】　池田　実
【特許出願人】
　【識別番号】　501125998
　【氏名又は名称】　池田　実
【代理人】
　【識別番号】　100089118
　【弁理士】
　【氏名又は名称】　酒井　宏明
【選任した代理人】
　【識別番号】　100113103
　【弁理士】
　【氏名又は名称】　香島　拓也
【先の出願に基づく優先権主張】
　【出願番号】　特願2001- 94347
　【出願日】　平成13年 3月28日
【手数料の表示】
　【予納台帳番号】　036711
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【物件名】　委任状　1

【援用の表示】　同日付提出の包括委任状

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報交換システム、情報通信端末、情報交換方法、プログラム、および、記録媒体

【特許請求の範囲】

【請求項１】　複数の要素を含む情報を送受信する情報通信端末を用いて上記情報を交換する情報交換システムにおいて、

送信側の情報通信端末は、

上記複数の要素の機密結合度を設定する機密結合度設定手段と、

上記機密結合度設定手段にて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定手段と、

上記分割ルール設定手段にて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割手段と、

上記分割手段にて分割された複数の上記疎結合情報、および、上記分割ルール設定手段にて設定された上記分割ルールを送信する送信手段と、

を備え、

受信側の情報通信端末は、

複数の上記疎結合情報、および、上記分割ルールを受信する受信手段と、

上記受信手段にて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成手段と、

を備えたことを特徴とする情報交換システム。

【請求項２】　上記送信手段は、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティング手段をさらに備え、

上記受信手段は、複数の上記疎結合情報を上記複数の伝送経路から受信することを特徴とする請求項１に記載の情報交換システム。

【請求項３】　上記送信側の情報通信端末は、

上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定手段と、

上記ネーミングルール設定手段にて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化手段と、

上記ネーミングルール設定手段にて設定された上記ネーミングルールを送信するネーミングルール送信手段と、

をさらに備え、

上記受信側の情報通信端末は、

上記ネーミングルールを受信するネーミングルール受信手段と、

上記ネーミングルール受信手段にて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換手段と、

をさらに備えたことを特徴とする請求項１に記載の情報交換システム。

【請求項４】　上記情報は、ＸＭＬにより記載されていることを特徴とする請求項１に記載の情報交換システム。

【請求項５】　上記機密結合度設定手段は、ＤＴＤに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項４に記載の情報交換システム。

【請求項６】　上記疎結合情報は、上記受信側の情報端末装置において再結合するための再結合情報を含み、

上記分割ルールは、上記疎結合情報と上記再結合情報との対応を特定するための情報を含むことを特徴とする請求項１に記載の情報交換システム。

【請求項７】　複数の要素を含む情報を送受信する情報通信端末において、

上記複数の要素の機密結合度を設定する機密結合度設定手段と、

上記機密結合度設定手段にて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定手段と、

上記分割ルール設定手段にて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割手段と、

上記分割手段にて分割された複数の上記疎結合情報、および、上記分割ルール設定手段にて設定された上記分割ルールを送信する送信手段と、

を備えたことを特徴とする情報通信端末。

【請求項８】　複数の上記疎結合情報、および、上記分割ルールを受信する受信手段と、

上記受信手段にて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成手段と、

をさらに備えたことを特徴とする請求項７に記載の情報通信端末。

【請求項９】　上記送信手段は、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティング手段をさらに備えたことを特徴とする請求項７に記載の情報通信端末。

【請求項１０】　上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定手段と、

上記ネーミングルール設定手段にて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化手段と、

上記ネーミングルール設定手段にて設定された上記ネーミングルールを送信するネーミングルール送信手段と、

をさらに備えたことを特徴とする請求項７に記載の情報通信端末。

【請求項１１】　上記ネーミングルールを受信するネーミングルール受信手段と、

上記ネーミングルール受信手段にて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換手段と、

をさらに備えたことを特徴とする請求項１０に記載の情報通信端末。

【請求項１２】　上記情報は、ＸＭＬにより記載されていることを特徴とする請求項７に記載の情報通信端末。

【請求項１３】　上記機密結合度設定手段は、ＤＴＤに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項１２に記載の情報通信端末。

【請求項１４】　上記疎結合情報は、受信側の情報端末装置において再結合するための再結合情報を含み、

上記分割ルールは、上記疎結合情報と上記再結合情報との対応を特定するための情報を含むことを特徴とする請求項７に記載の情報通信端末。

【請求項１５】　複数の要素を含む情報を送受信する情報通信端末を用いて上記情報を交換する情報交換システムを用いて実行される情報交換方法において、

送信側の情報通信端末において、上記複数の要素の機密結合度を設定する機密結合度設定ステップと、

上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、

上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、

上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを受信側の情報通信端末に対して送信する送信ステップと、

上記受信側の情報通信端末において、複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、

上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップと、

を含むことを特徴とする情報交換方法。

【請求項１６】　上記送信ステップは、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含み、

上記受信ステップは、複数の上記疎結合情報を上記複数の伝送経路から受信することを特徴とする請求項１５に記載の情報交換方法。

【請求項１７】　上記送信側の情報通信端末において、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルール

に基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを上記受信側の情報通信端末に対して送信するネーミングルール送信ステップと、

上記受信側の情報通信端末において、上記ネーミングルールを受信するネーミングルール受信ステップと、

上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップと、

をさらに含むことを特徴とする請求項１５に記載の情報交換方法。

【請求項１８】　上記情報は、ＸＭＬにより記載されていることを特徴とする請求項１５に記載の情報交換方法。

【請求項１９】　上記機密結合度設定ステップは、ＤＴＤに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項１８に記載の情報交換方法。

【請求項２０】　上記疎結合情報は、受信側の情報端末装置において再結合するための再結合情報を含み、

上記分割ルールは、上記疎結合情報と上記再結合情報との対応を特定するための情報を含むことを特徴とする請求項１５に記載の情報交換方法。

【請求項２１】　複数の要素を含む情報を送受信する情報通信端末に情報交換方法を実行させるプログラムにおいて、

上記複数の要素の機密結合度を設定する機密結合度設定ステップと、

上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、

上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、

上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分

割ルール設定ステップにおいて設定された上記分割ルールを送信する送信ステップと、

を含むことを特徴とするプログラム。

【請求項２２】　複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、

上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップと、

をさらに含むことを特徴とする請求項２１に記載のプログラム。

【請求項２３】　上記送信ステップは、

複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含むことを特徴とする請求項２１に記載のプログラム。

【請求項２４】　上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、

上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを送信するネーミングルール送信ステップと、

をさらに含むことを特徴とする請求項２１に記載のプログラム。

【請求項２５】　上記ネーミングルールを受信するネーミングルール受信ステップと、

上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップと、

をさらに含むことを特徴とする請求項２４に記載のプログラム。

【請求項２６】　上記情報は、ＸＭＬにより記載されていることを特徴とする請求項２１に記載のプログラム。

【請求項２７】　上記機密結合度設定ステップは、ＤＴＤに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする請求項２６に記載のプログラム。

【請求項２８】　上記疎結合情報は、受信側の情報端末装置において再結合するための再結合情報を含み、

上記分割ルールは、上記疎結合情報と上記再結合情報との対応を特定するための情報を含むことを特徴とする請求項２１に記載のプログラム。

【請求項２９】　請求項２１～２８のいずれか一つに記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報交換システム、情報通信端末、情報交換方法、プログラム、および、記録媒体に関し、特に、ＸＭＬにより記載された情報を送受信する情報交換システム、情報通信端末、情報交換方法、プログラム、および、記録媒体に関する。

【０００２】

【従来の技術】

インターネットは、利用者にとって極めて安価かつ容易に利用できる通信手段である。しかし、インターネットは、元来オープンなコミュニケーションのために作られ、利用されてきたものであるため、Ｂ２Ｂ（Ｂｕｓｉｎｅｓｓ　ｔｏ　Ｂｕｓｉｎｅｓｓ）の企業同士の取引などにおける企業情報や医療情報など秘匿性を要求される分野の情報交換手段には不向きである。そのため、これまでにインターネットの欠点を補い通信の安全性を確保するためのセキュリティ手段がいくつか開発されている。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来のインターネットにおけるセキュリティ手段は、導入が高価であり、複雑で手軽に利用できるものではなかったという問題点を有していた。

【０００４】

また、インターネットで広く用いられる比較的導入が容易なＳＳＬ（Ｓｅｃｕ

ｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）等の簡易な暗号システムを用いる場合には、第３者により比較的容易に暗号鍵を見破られる恐れがあるという問題点を有していた。

【０００５】

また、Ｂ２Ｂ等の情報交換においては、WWWコンソーシアム（Ｗ３Ｃ）が標準化を進めているＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）をデータの記述言語として用いる場合が多くなっている。ＸＭＬにより作成される情報は、要素（ｅｌｅｍｅｎｔ）を基本単位とする。「要素」は、要素に関連付けられた名前であって開始タグと終了タグの両方に記述される「要素名（ｅｌｅｍｅｎｔ　ｎａｍｅ）」、要素に関連付けられた内容であって開始タグと終了タグの間に記述される「要素内容（ｅｌｅｍｅｎｔ　ｃｏｎｔｅｎｔ）」、および、任意に指定される「属性（ａｔｔｒｉｂｕｔｅ）」からなる。ここで、要素は、ＤＴＤ（Ｄｏｃｕｍｅｎｔ　Ｔｙｐｅ　Ｄｅｆｉｎｉｔｉｏｎ）において定義される。すなわち、ＸＭＬは、情報（文書）の構造等をＤＴＤという文書型定義ファイルにして交換することができる。これにより、利用者は、情報交換される文書の表現方法の指定や文章中の文字列に意味を付加するような独自のタグを作成して用いることができる。このようにＸＭＬは高度な構造表現と明快な内容表現力を備えている。

【０００６】

しかしながら、このように優れた性質をもつＸＭＬであるが、逆に漏洩した場合は、その情報内容の解析が他の表現手段よりも容易となる。すなわち、ＸＭＬを用いた情報交換は、第三者がＤＴＤとＸＭＬ文書により情報（文書）の内容を容易に推測することができるので、ＨＴＭＬを用いた情報交換に比べて、第三者により情報交換される情報（文書）の内容を知られる可能性は高くなるという問題点がある。

【０００７】

このように、従来のシステム等は数々の問題点を有しており、その結果、利用者のいずれにとっても、利便性が悪く、また、セキュリティが悪いものであった。

本発明は上記問題点に鑑みてなされたもので、比較的手軽な暗号化のような機密保護に加えて、万一それが破られても情報の秘匿性の保持を可能とするものであり、オープンなインターネットを利用しつつ秘匿性が高い情報の交換を安価に実現することのできる、情報交換システム、情報通信端末、情報交換方法、プログラム、および、記録媒体を提供することを目的としている。

【０００８】

【課題を解決するための手段】

このような目的を達成するため、請求項１に記載の情報交換システムは、複数の要素を含む情報を送受信する情報通信端末を用いて上記情報を交換する情報交換システムにおいて、送信側の情報通信端末は、上記複数の要素の機密結合度を設定する機密結合度設定手段と、上記機密結合度設定手段にて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定手段と、上記分割ルール設定手段にて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割手段と、上記分割手段にて分割された複数の上記疎結合情報、および、上記分割ルール設定手段にて設定された上記分割ルールを送信する送信手段とを備え、受信側の情報通信端末は、複数の上記疎結合情報、および、上記分割ルールを受信する受信手段と、上記受信手段にて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成手段とを備えたことを特徴とする。

【０００９】

このシステムによれば、送信側の情報通信端末は、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の上記疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信し、受信側の情報通信端末は、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

【００１０】

また、請求項２に記載の情報交換システムは、請求項１に記載の情報交換シス

テムにおいて、上記送信手段は、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティング手段をさらに備え、上記受信手段は、複数の上記疎結合情報を上記複数の伝送経路から受信することを特徴とする。

【００１１】

これは送信手段の一例を一層具体的に示すものである。このシステムによれば、複数の疎結合情報を複数の伝送経路を用いて送信し、複数の疎結合情報を複数の伝送経路から受信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

【００１２】

また、請求項３に記載の情報交換システムは、請求項１に記載の情報交換システムにおいて、上記送信側の情報通信端末は、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定手段と、上記ネーミングルール設定手段にて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化手段と、上記ネーミングルール設定手段にて設定された上記ネーミングルールを送信するネーミングルール送信手段とをさらに備え、上記受信側の情報通信端末は、上記ネーミングルールを受信するネーミングルール受信手段と、上記ネーミングルール受信手段にて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換手段とをさらに備えたことを特徴とする。

【００１３】

このシステムによれば、送信側の情報通信端末は、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にするとともに、設定されたネーミングルールを送信する。受信側の情報通信端末は、ネーミングルールを受信するとともに、受信したネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信され

る情報の秘匿性をさらに高めることができる。

【００１４】

また、請求項４における情報交換システムは、請求項１に記載の情報交換システムにおいて、情報がＸＭＬにより記載されたものであることを特徴にする。

【００１５】

これは情報の一例を一層具体的に示すものである。このシステムによれば、情報がＸＭＬにより記載されたものであるので、ＸＭＬデータの分解・再構成の容易性を活かしてＸＭＬデータの機密結合度を下げ、秘匿性を高めることができる。

【００１６】

請求項５に記載の情報交換システムは、請求項４に記載の情報交換システムにおいて、上記機密結合度設定手段は、ＤＴＤに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

【００１７】

これは機密結合度設定手段の一例を一層具体的に示すものである。このシステムによれば、ＤＴＤに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、ＤＴＤに定義されたＸＭＬ情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

【００１８】

請求項６に記載の情報交換システムは、請求項１に記載の情報交換システムにおいて、上記疎結合情報は、上記受信側の情報端末装置において再結合するための再結合情報を含み、上記分割ルールは、上記疎結合情報と上記再結合情報との対応を特定するための情報を含むことを特徴とする。

【００１９】

これは疎結合情報の一例を一層具体的に示すものである。このシステムによれば、疎結合情報は、受信側の情報端末装置において再結合するための再結合情報を含み、分割ルールは、疎結合情報と再結合情報との対応を特定するための情報を含むので、分割された疎結合情報の再結合を媒介するための再結合情報を追加

することにより、情報の機密性をさらに高めることができる。

【００２０】

すなわち、乱数等により生成される再結合情報を疎結合情報に付加することにより、第三者が疎結合情報を見たときに、その内容の推定を困難にすることができる。また、どの再結合情報をどの疎結合情報に付加したかを分割ルールにおいて定義することにより、受信側の情報通信端末では、再結合情報に基づいて元の情報に再構成することができるようになる。

【００２１】

また、本発明は情報通信端末に関するものであり、請求項７に記載の情報通信端末は、複数の要素を含む情報を送受信する情報通信端末において、上記複数の要素の機密結合度を設定する機密結合度設定手段と、上記機密結合度設定手段にて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定手段と、上記分割ルール設定手段にて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割手段と、上記分割手段にて分割された複数の上記疎結合情報、および、上記分割ルール設定手段にて設定された上記分割ルールを送信する送信手段とを備えたことを特徴とする。

【００２２】

この端末によれば、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信するので、送受信される情報の秘匿性を高めることができる。

【００２３】

また、請求項８に記載の情報通信端末は、請求項７に記載の情報通信端末において、複数の上記疎結合情報、および、上記分割ルールを受信する受信手段と、上記受信手段にて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成手段とをさらに備えたことを特徴とする。

【００２４】

この端末によれば、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

【００２５】

また、請求項９に記載の情報通信端末は、請求項７に記載の情報通信端末において、上記送信手段は、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティング手段をさらに備えたことを特徴とする。

【００２６】

これは送信手段の一例を一層具体的に示すものである。この端末によれば、送信手段は、複数の疎結合情報を複数の伝送経路を用いて送信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

【００２７】

また、請求項１０に記載の情報通信端末は、請求項７に記載の情報通信端末において、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定手段と、上記ネーミングルール設定手段にて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化手段と、上記ネーミングルール設定手段にて設定された上記ネーミングルールを送信するネーミングルール送信手段とをさらに備えたことを特徴とする。

【００２８】

この端末によれば、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを送信するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【００２９】

また、請求項１１に記載の情報通信端末は、請求項１０に記載の情報通信端末

において、上記ネーミングルールを受信するネーミングルール受信手段と、上記ネーミングルール受信手段にて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換手段とをさらに備えたことを特徴とする。

【００３０】

この端末によれば、ネーミングルールを受信し、受信した上記ネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【００３１】

また、請求項１２に記載の情報通信端末は、請求項７に記載の情報通信端末において、上記情報は、ＸＭＬにより記載されていることを特徴とする。

【００３２】

これは情報の一例を一層具体的に示すものである。このシステムによれば、情報は、ＸＭＬにより記載されているので、ＸＭＬデータの分解・再構成の容易性を活かしてＸＭＬデータの機密結合度を下げ、秘匿性を高めることができる。

【００３３】

また、請求項１３に記載の情報通信端末は、請求項１２に記載の情報通信端末に　おいて、上記機密結合度設定手段は、ＤＴＤに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

【００３４】

これは機密結合度設定手段の一例を一層具体的に示すものである。このシステムによれば、ＤＴＤに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、ＤＴＤに定義されたＸＭＬ情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

【００３５】

請求項１４に記載の情報通信端末は、請求項７に記載の情報通信端末において

、上記疎結合情報は、上記受信側の情報端末装置において再結合するための再結合情報を含み、上記分割ルールは、上記疎結合情報と上記再結合情報との対応を特定するための情報を含むことを特徴とする。

【００３６】

これは疎結合情報の一例を一層具体的に示すものである。この装置によれば、疎結合情報は、受信側の情報端末装置において再結合するための再結合情報を含み、分割ルールは、疎結合情報と再結合情報との対応を特定するための情報を含むので、分割された疎結合情報の再結合を媒介するための再結合情報を追加することにより、情報の機密性をさらに高めることができる。

【００３７】

すなわち、乱数等により生成される再結合情報を疎結合情報に付加することにより、第三者が疎結合情報を見たときに、その内容の推定を困難にすることができる。また、どの再結合情報をどの疎結合情報に付加したかを分割ルールにおいて定義することにより、受信側の情報通信端末では、再結合情報に基づいて元の情報に再構成することができるようになる。

【００３８】

また、本発明は情報交換方法に関するものであり、請求項１５に記載の情報交換方法は、複数の要素を含む情報を送受信する情報通信端末を用いて上記情報を交換する情報交換システムを用いて実行される情報交換方法において、送信側の情報通信端末において、上記複数の要素の機密結合度を設定する機密結合度設定ステップと、上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを受信側の情報通信端末に対して送信する送信ステップと、上記受信側の情報通信端末において、複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結

合情報から上記情報を再構成する再構成ステップとを含むことを特徴とする。

【００３９】

この方法によれば、送信側の情報通信端末において、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを受信側の情報通信端末に対して送信し、受信側の情報通信端末において、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

【００４０】

また、請求項１６に記載の情報交換方法は、請求項１５に記載の情報交換方法において、上記送信ステップは、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含み、上記受信ステップは、複数の上記疎結合情報を上記複数の伝送経路から受信することを特徴とする。

【００４１】

これは送信ステップの一例を一層具体的に示すもので、この方法によれば、複数の疎結合情報を複数の伝送経路を用いて送信し、複数の疎結合情報を複数の伝送経路から受信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

【００４２】

また、請求項１７に記載の情報交換方法は、請求項１５に記載の情報交換方法において、上記送信側の情報通信端末において、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを上記受信側の情報通信端末に対して送信するネーミングルール送信ステップと、上記受信側

の情報通信端末において、上記ネーミングルールを受信するネーミングルール受信ステップと、上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップとをさらに含むことを特徴とする。

【００４３】

この方法によれば、送信側の情報通信端末において、要素の名称を別の名称とするためのネーミングルールを設定し、設定された上記ネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを受信側の情報通信端末に対して送信し、受信側の情報通信端末において、ネーミングルールを受信し、受信したネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【００４４】

また、請求項１８における情報交換方法は、請求項１５に記載の情報交換方法において、情報がＸＭＬにより記載されたものであることを特徴とする。

【００４５】

これは情報の一例を一層具体的に示すものである。この方法によれば、情報がＸＭＬにより記載されたものであるので、ＸＭＬデータの分解・再構成の容易性を活かしてＸＭＬデータの機密結合度を下げ、秘匿性を高めることができる。

【００４６】

また、請求項１９に記載の情報交換方法は、請求項１８に記載の情報交換方法において、上記機密結合度設定ステップは、ＤＴＤに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

【００４７】

これは機密結合度設定ステップの一例を一層具体的に示すものである。この方法によれば、ＤＴＤに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、ＤＴＤに定義さ

れたＸＭＬ情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

【００４８】

請求項２０に記載の情報交換方法は、請求項１５に記載の情報交換方法において、上記疎結合情報は、上記受信側の情報端末装置において再結合するための再結合情報を含み、上記分割ルールは、上記疎結合情報と上記再結合情報との対応を特定するための情報を含むことを特徴とする。

【００４９】

これは疎結合情報の一例を一層具体的に示すものである。この方法によれば、疎結合情報は、受信側の情報端末装置において再結合するための再結合情報を含み、分割ルールは、疎結合情報と再結合情報との対応を特定するための情報を含むので、分割された疎結合情報の再結合を媒介するための再結合情報を追加することにより、情報の機密性をさらに高めることができる。

【００５０】

すなわち、乱数等により生成される再結合情報を疎結合情報に付加することにより、第三者が疎結合情報を見たときに、その内容の推定を困難にすることができる。また、どの再結合情報をどの疎結合情報に付加したかを分割ルールにおいて定義することにより、受信側の情報通信端末では、再結合情報に基づいて元の情報に再構成することができるようになる。

【００５１】

また、本発明は、情報通信端末に情報交換方法を実行させるプログラムに関するものであり、請求項２１に記載のプログラムは、複数の要素を含む情報を送受信する情報通信端末に情報交換方法を実行させるプログラムにおいて、上記複数の要素の機密結合度を設定する機密結合度設定ステップと、上記機密結合度設定ステップにおいて設定された上記機密結合度に基づいて、上記情報を複数の疎結合情報に分割するための分割ルールを設定する分割ルール設定ステップと、上記分割ルール設定ステップにおいて設定された上記分割ルールに基づいて、上記情報を複数の上記疎結合情報に分割する分割ステップと、上記分割ステップにおいて分割された複数の上記疎結合情報、および、上記分割ルール設定ステップにおいて設定された上記分割ルールを送信する送信ステップとを含むことを特徴とす

る。

【００５２】

このプログラムによれば、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の上記疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信するので、送受信される情報の秘匿性を高めることができる。

【００５３】

また、請求項２２に記載のプログラムは、請求項２１に記載のプログラムにおいて、複数の上記疎結合情報、および、上記分割ルールを受信する受信ステップと、上記受信ステップにおいて受信した上記分割ルールに基づいて、複数の上記疎結合情報から上記情報を再構成する再構成ステップとをさらに含むことを特徴とする。

【００５４】

このプログラムによれば、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

【００５５】

また、請求項２３に記載のプログラムは、請求項２１に記載のプログラムにおいて、上記送信ステップは、複数の上記疎結合情報を複数の伝送経路を用いて送信するマルチルーティングステップをさらに含むことを特徴とする。

【００５６】

これは送信ステップの一例を一層具体的に示すものである。このプログラムによれば、複数の疎結合情報を複数の伝送経路を用いて送信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

【００５７】

また、請求項２４に記載のプログラムは、請求項２１に記載のプログラムにお

いて、上記要素の名称を別の名称とするためのネーミングルールを設定するネーミングルール設定ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールに基づいて、上記情報の上記要素の名称を別の名称にする別名化ステップと、上記ネーミングルール設定ステップにおいて設定された上記ネーミングルールを送信するネーミングルール送信ステップとをさらに含むことを特徴とする。

【００５８】

このプログラムによれば、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを送信するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【００５９】

また、請求項２５に記載のプログラムは、請求項２４に記載のプログラムにおいて、上記ネーミングルールを受信するネーミングルール受信ステップと、上記ネーミングルール受信ステップにおいて受信した上記ネーミングルールに基づいて、別名化された上記情報の上記要素の名称を元の名称に変換する名称変換ステップとをさらに含むことを特徴とする。

【００６０】

このプログラムによれば、ネーミングルールを受信し、受信したネーミングルールに基づいて、別名化された情報の上記要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【００６１】

また、請求項２６に記載のプログラムは、請求項２１に記載のプログラムにおいて、上記情報は、ＸＭＬにより記載されていることを特徴とする。

【００６２】

これは情報の一例を一層具体的に示すものである。このプログラムによれば、情報は、ＸＭＬにより記載されているので、ＸＭＬデータの分解・再構成の容易性を活かしてＸＭＬデータの機密結合度を下げ、秘匿性を高めることができる。

【００６３】

また、請求項２７に記載のプログラムは、請求項２６に記載のプログラムにおいて、上記機密結合度設定ステップは、ＤＴＤに定義されている上記要素について、上記要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定することを特徴とする。

【００６４】

これは機密結合度設定ステップの一例を一層具体的に示すものである。このプログラムによれば、ＤＴＤに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、ＤＴＤに定義されたＸＭＬ情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

【００６５】

請求項２８に記載のプログラムは、請求項２１に記載のプログラムにおいて、上記疎結合情報は、上記受信側の情報端末装置において再結合するための再結合情報を含み、上記分割ルールは、上記疎結合情報と上記再結合情報との対応を特定するための情報を含むことを特徴とする。

【００６６】

これは疎結合情報の一例を一層具体的に示すものである。このプログラムによれば、疎結合情報は、受信側の情報端末装置において再結合するための再結合情報を含み、分割ルールは、疎結合情報と再結合情報との対応を特定するための情報を含むので、分割された疎結合情報の再結合を媒介するための再結合情報を追加することにより、情報の機密性をさらに高めることができる。

【００６７】

すなわち、乱数等により生成される再結合情報を疎結合情報に付加することにより、第三者が疎結合情報を見たときに、その内容の推定を困難にすることができる。また、どの再結合情報をどの疎結合情報に付加したかを分割ルールにおい

て定義することにより、受信側の情報通信端末では、再結合情報に基づいて元の情報に再構成することができるようになる。

【００６８】

また、本発明は記録媒体に関するものであり、請求項２９に記載の記録媒体は、上記請求項２１～２８のいずれか一つに記載されたコンピュータに実行させるためのプログラムを記録したことを特徴とする。

【００６９】

この記録媒体によれば、当該記録媒体に記録されたプログラムをコンピュータに読み取らせて実行することによって、請求項２１～２８のいずれか一つに記載されたプログラムにより実現される情報交換方法をコンピュータを利用して実現することができ、これら各方法と同様の効果を得ることができる。

【００７０】

【発明の実施の形態】

以下に、本発明にかかる情報交換システム、情報通信端末、情報交換方法、プログラム、および、記録媒体の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

特に、以下の実施の形態においては、本発明を、ＸＭＬに適用した例について説明するが、この場合に限られず、ＳＧＭＬやＨＴＭＬ等のごとく、所定の情報に対してタグ等により属性等を定義することができる全ての記述言語において、同様に適用することできる。

【００７１】

（本システムの概要）

以下、本システムの概要について説明し、その後、本システムの構成および処理等について詳細に説明する。図１は本システムの全体構成の一例を示すブロック図であり、また、図２は本システムの概要を示す概念図であり、それぞれ該システム構成のうち本発明に関係する部分のみを概念的に示している。

【００７２】

本システムは、図１に示すように、概略的に、各情報通信端末１００がネットワーク３００を介して通信可能に接続して構成されている。ここで、情報通信端

末１００は、既知のパーソナルコンピュータ、ワークステーション、家庭用ゲーム装置、インターネットＴＶ、ＰＨＳ端末、携帯端末、移動体通信端末、ＰＤＡ等の情報処理端末等の情報処理装置にプリンタやモニタやイメージスキャナ等の周辺装置を必要に応じて接続し、該情報処理装置にウェブ情報のブラウジング機能や電子メール機能や後述する各機能を実現させるソフトウェア（プログラム、データ等を含む）を実装することにより実現してもよい。

【００７３】

このシステムは、概略的に、以下の基本的特徴を有する。すなわち、情報通信端末１００から他の情報通信端末１００に対して、情報がネットワーク３００を介して提供される。

このうち、情報は、一例としてＸＭＬにより記述されたものであり、ＤＴＤ（文書型定義）にて定義されたタグ等のメタデータを含む。これらの情報は、情報通信端末１００、または、他の装置により生成され、情報通信端末１００に蓄積される。

【００７４】

本システムは、図２に示すように、送信側の情報通信端末１００が設定する分解ルールおよび再構成ルールにより、情報が送信側の情報通信端末１００において分解され、受信側の情報通信端末１００において再構成される。これにより、既存のシステムやアプリケーションに対して影響を与えず、かつ簡易に導入することができ、高い安全性を得ることができるようになる。

以下に、本システムの情報通信端末１００における分解ルールおよび再構成ルールの設定について、その概念を説明する。

【００７５】

（１）機密結合度

まず始めに、「機密結合度」の概念を導入する。

上述したように、ＸＭＬにより作成される情報は、ＤＴＤにおいて定義された要素（ｅｌｅｍｅｎｔ）を基本単位とする。上述したように、ＤＴＤにおいて、各要素の名称、内容、属性等が定義される。

【００７６】

ここで、交換情報を構成する要素（ｅｌｅｍｅｎｔ）の組合せにより、利用者が期待する機密レベルが異なることが多い。たとえば、企業情報のうち、企業名や社長名は、公開されている情報であるため、その要素を組み合わせた情報は、機密レベルが低い（単なる公開されている情報の結合に過ぎないため）。また、欠損額等の非公開の要素について、その情報のみを交換する場合には、漏洩されても何処の企業の欠損額であるかは特定できないため実害は少ない。

【００７７】

しかしながら、非公開の要素と公開された要素とを結合させた場合には、その内容が漏洩されると公開情報に基づいて非公開の要素が詳細に特定されてしまう恐れが強い。

【００７８】

そこで、本システムでは、特定の要素の組合せ毎に「機密結合度」を定義することにより、要素の結合を機密レベルの観点からチェックする。

【００７９】

すなわち、本システムは、ＤＴＤにおいて定義された各要素について、その要素の名称、内容、属性等に基づいて他の要素と組み合わせた場合の機密結合度を指定する。「機密結合度」は、複数の要素を結合させた場合に、その要素の組合せにより情報の機密性が高くなるか否かを示す値であり、例えば、機密性が高まるにつれて高い数値を設定する。例えば、各要素の名称、内容、属性等をモニタに表示して、利用者に表示された要素の組み合わせ毎に機密結合度を指定させてもよく、また、情報通信端末１００が各要素の名称、内容、属性等の情報に基づいて自動的に機密結合度を指定してもよい。

【００８０】

ここで、情報通信端末１００が各要素の名称、内容、属性等の情報に基づいて自動的に機密結合度を指定する場合の一例を説明する。各要素に必須の属性として、要素内容が公開情報か否かに関する情報（以下「公開属性」という）をＤＴＤにおいて定義する。そして、情報通信端末１００は、各要素の公開属性を判断して、公開情報となる要素と非公開情報となる要素との機密結合度を、自動的に高く設定する。

【００８１】

なお、機密結合度は、２つの要素の関係に限定されるものではなく、例えば、３つ以上の要素が組み合わさって初めて機密性が高くなる場合には、３つ以上の要素の組み合わせで機密度を高く設定する。

【００８２】

図６は、本システムにおける機密結合度の定義の一例を示す概念図である。

本図において、オリジナルのＸＭＬの情報６０１は、要素として企業名と社長名と当季欠損額とを含んでいる。ここで、利用者等は、企業名と社長の名前は公示されているものであり機密結合度が低いと定義する。一方、企業の欠損額は秘匿性が高いので企業名と企業の欠損額の組合せは機密結合度が高いと定義する。

【００８３】

仮に、この３つの要素を、機密結合度の高・低に従って分割する分割ルールを生成し、この分割ルールに基づいて、企業名および社長名の組合せを含む情報６０２と、欠損額の情報６０３とに２分割すると、この両者の機密結合度は低下する。つまり、２つに分割された情報は、両者の対応関係が明らかにならない限り機密的な結合が疎であり、全体として機密結合度が低くなる。

【００８４】

本システムは、ＸＭＬデータの分解・再構成の容易性を活かしてＸＭＬデータの機密結合度を下げ、秘匿性を高めるものである。ここで、結合度を下げる目的で分割したＸＭＬデータを「疎結合ＸＭＬデータ」と称する。また、結合ルール６０４（すなわち、疎結合ＸＭＬと密結合ＸＭＬとの変換ルールであり、後述する分解ルールおよび再構成ルールとなるものである）を、リポジットリやＤＴＤファイルや他のファイルに記録して相互に交換することにより、当事者同士は情報を再構成し確認することができる。

【００８５】

（２）疎結合ＸＭＬデータのマルチルーティング

上述したように、機密結合度が下げられて生成された複数の疎結合ＸＭＬデータは、それぞれを別の通信路を用いて情報の交換を行うことにより、両者の対応関係を隠蔽し、機密の保護をより完全にすることができる。このように、本シス

テムでは、生成した疎結合ＸＭＬデータを、別の通信路を用いてマルチルーティングすることにより、セキュリティを高めている。ここで、ルーティング数は可変とする。

【００８６】

図７は、本発明の疎結合ＸＭＬデータのマルチルーティングの概要を示す概念図である。

本図に示すように、オリジナルのＸＭＬデータは、ＤＴＤと、利用者等に指定された機密結合度とから生成されたルールに従って（ステップＳ７０１）、複数の疎結合ＸＭＬに分解され（ステップＳ７０３）、複数の伝送経路を経て送信側に送られる（ステップＳ７０４）。

受信側は、複数の伝送経路から受け取った疎結合ＸＭＬデータを、別途送られてきているルールに基いて（ステップＳ７０２）、再構成し、オリジナルＸＭＬと同一のＸＭＬデータを得る（ステップＳ７０５）。

【００８７】

（３）要素名の別名化

ＸＭＬは、上述したように高度な構造表現と明快な内容表現力を備えている。そのように優れた性質をもつＸＭＬではあるが、逆に漏洩した場合は、その情報内容の解析が他の表現手段よりずっと容易となる。特に、要素名は、運用上その要素の内容を直接的に示す場合が多いため、その要素名から要素内容を容易に推測することができる。

【００８８】

従って、本システムでは、要素名の別名化を行う。この別名化の機能は、オリジナルのＸＭＬから別の名称と構造を持つＸＭＬを生成するものである。この機能によりオリジナル情報の推定を困難にする。

【００８９】

図８は、本発明の要素名の別名化の概要を示す概念図である。

上述したように、密結合ＸＭＬデータから、疎結合ＸＭＬデータ（８０１および８０２）と、結合ルール８０３とが生成されると、要素名について別名化を行う。「別名化」とは、ネーミングルールに基づいて、要素名を対応する別名に置

換するこという。

【００９０】

例えば、本図に示すように、「企業名」を「ＡＡＡ」に、「社長名」を「ＢＢＢ」に、また、「当季欠損額」を「ＸＹＺ」に置換する対応表に基づいたネーミングルールを設定し、別名化したＸＭＬ（以下「別名ＸＭＬ」と称する）８０４および８０５を作成し、結合ルールとネーミングルールとを一組の情報８０６にして管理する。

【００９１】

ここで、ネーミングルールは、上述した対応表を用いた変換によるものでもよく、また、ハッシュ関数等の数学的アルゴリズムを用いた変換によるものでもよい。

【００９２】

（システム構成）

以下、このような基本的特徴を具現化するための、本システムの構成について説明する。

【００９３】

（システム構成－情報通信端末１００）

まず、情報通信端末１００の構成について説明する。図３は、本発明が適用される情報通信端末１００の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図３において情報通信端末１００は、概略的に、情報通信端末１００の全体を統括的に制御するＣＰＵ等の制御部１０２、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インタフェース部１０４、入出力装置（図示せず）に接続される入出力制御インタフェース部１０８、および、各種のデータを格納する記憶部１０６を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、この情報通信端末１００は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介して、ネットワーク３００に通信可能に接続されている。

【００９４】

記憶部１０６は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。情報通信端末１００の記憶部１０６には、例えば、ＤＴＤやＸＭＬデータやスキーマのリポジットリ、結合ルールやネーミングルール等の各種のルール情報等が格納される。

【００９５】

また、図３において、通信制御インタフェース部１０４は、情報通信端末１００とネットワーク３００（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インタフェース部１０４は、他の端末と通信回線を介してデータを通信する機能を有する。

【００９６】

また、図３において、入出力制御インタフェース部１０８は、入力装置や出力装置の制御を行う。ここで、出力装置としては、モニタ（家庭用テレビを含む）の他、スピーカを用いることができる（なお、以下においては出力装置をモニタとして記載する）。また、入力装置としては、キーボード、マウス、および、マイク等を用いることができる。また、モニタも、マウスと協働してポインティングデバイス機能を実現する。

【００９７】

また、図３において、制御部１０２は、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部１０２は、機能概念的に、設定モジュール１０２ａ、実行モジュール１０２ｂ、および、ＸＭＬミドルウェア１０２ｃを備えて構成されている。なお、これら各部によって行なわれる処理の詳細については、後述する。

【００９８】

（システム構成－情報通信端末１００のソフトウェア構成）

次に、このように構成された情報通信端末１００のソフトウェア構成について、図４を参照して説明する。図４は、本発明が適用される情報通信端末１００の

１０２において実行されるソフトウェア構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図４において情報通信端末１００は、概略的に、設定モジュール１０２ａと、実行モジュール１０２ｂと、ＸＭＬミドルウェア１０２ｃとを含んで構成される。

【００９９】

図４において、設定モジュール１０２ａは、上述した結合ルールやネーミングルール等のルールを設定する機能を有し、以下に説明する、ＤＴＤリポジットリと、ルールビルダと、ルール設定処理部とを含んで構成される。

【０１００】

（１）ＤＴＤリポジットリ

ＤＴＤリポジットリは、ＸＭＬデータのメタデータの記憶手段である。ここで、複数のＸＭＬビジネスデータを扱う利用環境を想定すると、ＤＴＤをまとめて体系的に管理・利用を行う仕組みが必要となる。ＤＴＤリポジットリは、大量のＤＴＤをネットワーク上で共同利用するための道具であり、ＤＴＤやスキーマ等を管理する。ＤＴＤリポジットリは、一般に、情報入出力インタフェース機能、記憶領域の管理機能を備えるソフトウェアにより構成される。

【０１０１】

（２）ルールビルダ

上述したように、データの利用者は、データ内容や機密のレベルを定め、それを機密結合度として指定する。ルールビルダは、利用者の指定内容とＤＴＤとを参照しながら結合ルールやネーミングルール等の各種のルールを自動的に生成する。

【０１０２】

（３）ルール設定処理部

ルール設定処理部は、モニタにルールの設定画面（例えば、各要素の名称、内容、属性等の表示領域と、各要素の機密結合度の入力領域とを含む画面）を表示して、利用者が各種のルールを入力装置を介して設定するための処理を行う。

【０１０３】

また、図４において実行モジュール１０２ｂは、ＸＭＬミドルウェア１０２ｃ

から受信した情報を、設定モジュール１０２ａにより設定された各種のルールに従って、処理を実行する機能を有し、以下に説明する、パーサと、デバイダと、ＩＰアロケータと、ＩＰ／ポートマネジャーと、サーバと、コンストラクタと、入出力コネクタとを含んで構成される。

【０１０４】

（１）パーサ

パーサは、Ｗ３ＣのＸＭＬ規格に準拠した構文解析を行い、トークンを作成して、デバイダに引き渡す機能を有する。すなわち、パーサは、テキストを解釈し、その論理的意味を判断し、その意味を表すプログラミングデータ構造を作成するソフトウェアプログラムである。なお、本システムは、ツリーベースのパーサであっても、イベントベースのパーサであってもよい。

また、受信時には、別名化された要素名をネーミングルールに基づいて元の要素名に変換する機能を有する。

【０１０５】

（２）デバイダ

デバイダは、設定モジュールが生成したルールに従って、ＸＭＬデータの分割を行う機能を有する。また、送信時には、要素名の別名化を行う機能を有する。

【０１０６】

（３）ＩＰアロケータ

ＩＰアロケータは、分割数に応じたＩＰの割当や、開放を行う機能を有する。

【０１０７】

（４）ＩＰ／ポートマネジャー

ＩＰ／ポートマネジャーは、ＩＰやポートを複数利用する際には資源を動的に割り当てることが必要となるため、これらの資源の監視と管理を行う機能を有する。

【０１０８】

（５）サーバ

サーバは、Ｗｅｂ、Ｆｔｐ、ｓｍｔｐなどのサービスするプロトコルに対応するサーバ機能を有する。

【０１０９】

（６）コンストラクタ

コンストラクタは、パーサが生成したトークンを受け取り、再構成ルールに従ってＸＭＬデータを再構成する機能を有する。

【０１１０】

（７）入出力コネクタ

入出力コネクタは、実行モジュールの外側にあるアプリケーションシステムとのコミュニケーションを行う機能を有する。

【０１１１】

図４において、ＸＭＬミドルウェア１０２ｃは、ＸＭＬデータを処理するミドルウェアであり、利用者が実行するアプリケーションプログラムから、交換情報となるＸＭＬデータを実行モジュール１０２ｂに渡す機能を有する。また、実行モジュール１０２ｂにおいて他の情報通信端末１００から受信したＸＭＬデータをアプリケーションプログラムに渡す機能を有する。

【０１１２】

（情報通信端末１００における情報の流れ）

このように構成された情報通信端末１００における情報の流れを図５、図９および図１０を用いて説明する。

【０１１３】

図５は、情報通信端末１００における情報の流れの概要を説明する概念図である。以下に、送信側の情報通信端末１００の情報の流れと、受信側の情報通信端末１００の情報の流れに分けて説明する。

【０１１４】

（１）送信側の情報通信端末１００

まず、前提として、設定モジュール１０２ａにおいて、疎結合ＸＭＬの生成に用いる各種のルールを生成する。ここで、図１０は、設定モジュール１０２ａにおける疎結合ＸＭＬの生成に用いる各種ルールの生成の概要を示す概念図である。

【０１１５】

例えば、企業情報に関するＸＭＬ文書を処理する場合を一例に説明すると、ルール設定処理部は、ＤＴＤリポジットリから企業情報用のＤＴＤを参照して、ルール設定画面等を作成し、データ所有者による各要素の機密結合度の指定を行わせる。ルールビルダは、データ所有者が行った指定内容に基づいて、結合ルールおよびネーミングルール（情報通信端末１００１および情報通信端末１００２）を自動生成する。なお、作成した各種のルールは、受信側の情報通信端末１００に対して送信される。

【０１１６】

ついで、図５に示すように、ユーザアプリケーションで作成されたオリジナルＸＭＬデータは、ＸＭＬミドルウェア１０２ｃを介して、実行モジュール１０２ｂの入出力コネクタに送信される（ステップＳ５０１）。

【０１１７】

入出力コネクタは、オリジナルＸＭＬデータを、パーサに送信する（ステップＳ５０２）。

【０１１８】

ついで、パーサは、オリジナルＸＭＬデータの構文解析を行い、トークンを生成して、デバイダに送信する（ステップＳ５０３）。

【０１１９】

ついで、デバイダは、設定モジュール１０２ａが生成したルールに従って、ＸＭＬデータの分割を行い、また上述したように要素名の別名化を行い、疎結合ＸＭＬデータを作成する。

【０１２０】

ここで、図９は、デバイダにより実行される要素名の別名化、および、疎結合ＸＭＬデータの作成の一例を示す概念図である。本事例は、オリジナルＸＭＬ９０１に対して疎結合化を行い、２つのＸＭＬデータ９０２および９０３を生成する。同時にネーミングルールに従って別の要素名を設定している。第三者が、このような疎結合ＸＭＬからオリジナルＸＭＬを作り出すことは極めて難しい。

【０１２１】

再び図５に戻り、デバイダは、ＩＰアロケータの制御に基づいてＩＰの割り当

てを行い、また、ＩＰ／ポートマネジャーの制御により資源の割り当てを行う。そして、上述したマルチルーティングを実行するために、複数のＩＰアロケータに疎結合ＸＭＬデータを送信する（ステップＳ５０４）。

【０１２２】

ついで、各ＩＰアロケータはサーバに対して別の通信路を用いて受信側の情報通信端末１００に対して疎結合ＸＭＬデータを送信するように依頼する（ステップＳ５０５）。

【０１２３】

サーバは、各通信路を用いて、疎結合ＸＭＬデータを受信側の情報通信端末１００に対して送信する（ステップＳ５０６）。

【０１２４】

（２）受信側の情報通信端末１００

サーバは、ネットワーク３００を介して疎結合ＸＭＬを受信すると（ステップＳ５０７）、疎結合ＸＭＬをパーサに対して送信する（ステップＳ５０８）。

【０１２５】

ついで、パーサは、送信側の情報通信端末１００から受信したＤＴＤファイルや、各種のルールに基づいて、別名化された要素名の復元したのち、疎結合ＸＭＬの構文解析を行い、トークンを生成してコンストラクタに送信する（ステップＳ５０９）。

【０１２６】

ついで、コンストラクタは、結合ルールに基づいて、疎結合ＸＭＬからオリジナルＸＭＬを再構成して、入出力コネクタに送信する（ステップＳ５１０）。

【０１２７】

ついで、入出力コネクタは、再構成したＸＭＬデータを、ＸＭＬミドルウェア１０２ｃに送信すると、ＸＭＬミドルウェア１０２ｃは、ユーザアプリケーションにＸＭＬデータを送信する（ステップＳ５１１）。

【０１２８】

（システム構成－ネットワーク３００）

次に、図１のネットワーク３００の構成について説明する。ネットワーク３０

０は、情報通信端末１００を相互に接続する機能を有し、例えば、インターネット等である。

【０１２９】

（再結合情報を用いる実施形態）

インターネットを利用してカード決済やインターネットディビット決済をしようとすると、カード番号や口座番号やパスワードや取引金額を画面から入力しなければならない。その際、多くの人はインターネット上に秘密情報が流れることについて不安を感じる。オープンな環境であり、かつ目的や内容や質の異なる雑多な情報に満ちているインターネット上で、このような秘匿性の高い情報を扱うには、こうした利用者側の不安を取り除き、安心して電子商取引などが行える環境を整備しなければならない。

【０１３０】

現在、インターネット上で最も普及しているＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）などの一般的な暗号化の手法は、クラッカーにより万が一暗号化が破られると、ＩＤやパスワードなどの全ての機密情報がクラッカーに開示される結果になる。

【０１３１】

そこで、そうした機密度の高い情報を本発明の機密結合度に従って分割し伝送することによって、何れかの部分情報が開示されても、他の口座情報などの情報が完全に再現されるのを阻止し、第三者の不正な侵入や決済の実行を未然に防ぐことが極めて重要である。

【０１３２】

ここで、ＸＭＬデータ等で記載されたビジネストランザクションなどの情報は、多数の要素を持ち、また、構造も複雑なため、複数に分割された疎結合情報を受信側で再結合する際には、相互の対応付けのための情報（再結合情報）が存在するのが一般的である。

【０１３３】

例えば、受発注データなどであれば、再結合情報として、企業コードなどの共通的な情報を用いることができる。

【０１３４】

一方、ＩＤやパスワードなどを送受信するための情報は、一般的に、要素数が２つまたは３つであり、構造も極めて単純なため、再結合に当たっては、そのまま分割して複数の経路から送っても、到着順に結合すると、元の情報を容易に推定することができ、受信側における安全な再結合が期待できない。

【０１３５】

そこで、本実施形態においては、オリジナルのＸＭＬデータに、受信側の情報通信端末１００における再結合の際に使用する共通要素または属性を再結合情報として送信側の情報通信端末１００で生成し、その再結合情報を原ＸＭＬデータに付加することにより、各疎結合ＸＭＬデータの対応関係を維持する。

【０１３６】

ここで、図１１は、再結合情報を用いて情報の分解および再構成を行う場合の一例を示す概念図である。図中で、白の四角形で表示されているのが情報通信端末間で送受信される情報（オリジナルＸＭＬ）に付加された再結合情報である。再結合情報は、元の情報であるオリジナルＸＭＬデータには存在しない情報であり、受信側で複数の疎結合ＸＭＬからオリジナルＸＭＬを再構成する際に正しい組み合せの相手を見つけるために、送信側で作成されてオリジナルＸＭＬに付加される。

【０１３７】

ここで、再結合情報は、できるだけ元の情報の推定を困難にするために、乱数など利用することが好ましい。

【０１３８】

以下に、再結合情報を用いて情報の分解および再構成を行う場合の一例を、図１２～図１９を参照して、詳細に説明する。本実施形態においては、オリジナルＸＭＬ情報としてカードデータを使用する場合を一例を示す。

【０１３９】

（１）オリジナルＸＭＬ情報（カード情報）

図１２は、カード情報を格納したオリジナルＸＭＬ情報の一例を示す図である。本図に示すように、オリジナルＸＭＬ情報は、カード番号、パスワードおよび

有効期限の各要素から構成されている。

【０１４０】

（２）分解／再構成ルール

図１３は、本実施形態における分解／再構成ルールの一例を示す図である。本図において、＠ｒａｎｄｏｍは、乱数発生関数であり、＠ｔｉｍｅｄａｙは、現在時間を取得する関数である。本実施形態における分解／再構成ルールは、この２つの関数によって、現在時間をシーズとするユニークな乱数を発生し、その値を変数＠ｎｕｍに格納する。

【０１４１】

本図において、再構成の際の、疎結合ＸＭＬデータの再結合の指示は、

ｂｉｎｄｉｎｇ＝“ａｂｃ／ｚｚｚ：ｘｙｚ／ｈｅｄ：ｍｉｘ／ｉｆｓ”

によって規定している。

すなわち、本図においては、３つの要素が再結合の媒介キー（再結合情報）であることを示しており、具体的には、疎結合ＸＭＬ＜ａｂｃ＞においては、要素＜ｚｚｚ＞が媒介キー（再結合情報）であり、また、次の疎結合ＸＭＬ＜ｘｙｚ＞においては、要素＜ｈｅｄ＞が媒介キー（再結合情報）であり、さらに、次の疎結合ＸＭＬ＜ｍｉｘ＞においては、要素＜ｉｆｓ＞が媒介キー（再結合情報）であることを示している。

【０１４２】

なお、図１３において、下線が付した語は、予約語であり、その意味と記法を本システム内で予め定めておく。

【０１４３】

また、図１３において、関数（＠のついた語）の実行や代入は、送信側の情報通信端末１００で実行され、その値を確定する。そして、確定した値をオリジナルＸＭＬデータに埋め込んだ後、上述した分割方法を用いて疎結合ＸＭＬデータに分割して、該疎結合ＸＭＬデータを受信側に対して送信する。なお、受信側の情報通信端末１００では、この分解／再構成ルールを、結合を媒介するキーの要

素である再結合情報が何れであるかを知るために参照するため、および、別名化された要素名の逆変換のために利用し、関数等の実行は行わない。

【０１４４】

（３）疎結合ＸＭＬデータ

図１４は、本実施の形態の分解／再構成ルールに従って分解された疎結合ＸＭＬデータの一例を示す図である。本図においては、媒介キー（再結合情報）を、「ｇｊ５６ａ０２ｊ」とする場合に生成される疎結合ＸＭＬデータを示す。

【０１４５】

また、受信側の情報通信端末１００では、この３つの疎結合ＸＭＬを元に、分解／再構成ルールのｂｉｎｄｉｎｇで示された媒介キー（再結合情報）によってＸＭＬデータの再構成を行う。

【０１４６】

（４）受信側におけるオリジナルＸＭＬデータの再構成

受信側の情報通信端末１００では、同時に複数の疎結合ＸＭＬデータを受け付けなければならない。また、疎結合ＸＭＬデータは、非同期的に送られてくるので、複数の疎結合ＸＭＬデータを受信側の情報通信端末１００のメモリ上にプールして再構成を行う。

【０１４７】

ここで、図１５は、本実施の形態において受信側の情報通信端末１００のメモリ上にプールされる情報の一例を示す図である。本図に示すように、再構成用のバファープールにプールされる情報としては、オリジナルＸＭＬ情報にｂｉｎｄｉｎｇ要素を付加した情報とする。

【０１４８】

この領域を利用し、以下の手順で再構成を行う。

まず、図１６は、本実施の形態において初期状態のバファープールに格納される情報の一例を示す図である。図１６に示すように、初期状態におけるバファープールは、全ての要素が空値を持つＸＭＬデータである。

【０１４９】

ついで、疎結合ＸＭＬデータを受信した場合には、受信した疎結合ＸＭＬデー

タ中のｂｉｎｄｉｎｇキーと同一の値を持つｂｉｎｄｉｎｇ要素をバファープール中のＸＭＬデータから探し、見つかれば、疎結合ＸＭＬデータをプール中の該当する要素の値としてセットする。

【０１５０】

例えば、図１７に示すカード番号の疎結合ＸＭＬデータを受信した場合には、図１８に示すように、バファープール中の該当するカード番号要素に、カード番号「１２３４６７８９７９９」がセットされる。

【０１５１】

このような再構成を残りの２つの疎結合ＸＭＬデータに対しても同様に行う。

ここで、図１９は、全ての疎結合ＸＭＬデータを受信し、バファープール上の各要素にデータをセットした結果を示す図である。

【０１５２】

そして、最終的に、媒介キー（再結合情報）を除いたｍｙ－ｃａｒｄ要素だけを取り出し、完全なカード情報であるオリジナルＸＭＬデータを再現する。

【０１５３】

ここで、システムにおいて、時間を監視して一定時間を過ぎてもカード情報の３つの要素が完結しない場合は、不足部分の疎結合データの再送や再入力を促してもよい。

【０１５４】

また、本実施の形態で示した例では、説明の便宜ため、ソース形式のＸＭＬデータで説明したが、全ての操作はＸＭＬオブジェクト（ＤＯＭ）に対して行ってもよい。

【０１５５】

（他の実施の形態）

さて、これまで本発明の実施の形態について説明したが、本発明は、上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてよいものである。

【０１５６】

また、実施形態において説明した各処理のうち、自動的に行なわれるものとし

て説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行なわれるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。

この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種の登録データや検索条件等のパラメータを含む情報、画面例、データベース構成については、特記する場合を除いて任意に変更することができる。

【０１５７】

また、情報通信端末１００に関して、図示の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。

例えば、情報通信端末１００が備える処理機能、特に制御部にて行なわれる各処理機能については、その全部または任意の一部を、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）および当該ＣＰＵにて解釈実行されるプログラムにて実現することができ、あるいは、ワイヤードロジックによるハードウェアとして実現することも可能である。

【０１５８】

また、情報通信端末１００は、さらなる構成要素として、マウス等の各種ポインティングデバイスやキーボードやイメージスキャナやデジタイザ等から成る入力装置（図示せず）、入力データのモニタに用いる表示装置（図示せず）、システムクロックを発生させるクロック発生部（図示せず）、および、各種処理結果その他のデータを出力するプリンタ等の出力装置（図示せず）を備えてもよい。

【０１５９】

記憶部に格納される各種のデータは、ＲＡＭ、ＲＯＭ等のメモリ装置、ハードディスク等の固定ディスク装置、フレキシブルディスク、光ディスク等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【０１６０】

さらに、情報通信端末１００の分散・統合の具合的形態は図示のものに限られず、その全部または一部を、各種の負荷等に応じた任意の単位で、機能的または物理的に分散・統合して構成することができる。例えば、各データを独立したデ

ータベース装置として独立に構成してもよく、また、処理の一部をＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）を用いて実現してもよい。

【０１６１】

この情報通信端末１００の制御部は、その全部または任意の一部を、ＣＰＵおよび当該ＣＰＵにて解釈実行されるプログラムにて実現することができる。すなわち、記憶部には、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）と協働してＣＰＵに命令を与え、各種処理を行うためのコンピュータプログラムが記録されている。このコンピュータプログラムは、ＲＡＭにロードされることによって実行され、ＣＰＵと協働して制御部を構成する。

【０１６２】

しかしながら、このコンピュータプログラムは、情報通信端末１００に対して任意のネットワークを介して接続されたアプリケーションプログラムサーバに記録されてもよく、必要に応じてその全部または一部をダウンロードすることも可能である。このあるいは、各制御部の全部または任意の一部を、ワイヤードロジック等によるハードウェアとして実現することも可能である。

【０１６３】

また、本発明にかかるプログラムを、コンピュータ読み取り可能な記録媒体に格納することもできる。ここで、この「記録媒体」とは、フロッピーディスク、光磁気ディスク、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等の任意の「可搬用の物理媒体」や、各種コンピュータシステムに内蔵されるＲＯＭ、ＲＡＭ、ＨＤ等の任意の「固定用の物理媒体」、あるいは、ＬＡＮ、ＷＡＮ、インターネットに代表されるネットワークを介してプログラムを送信する場合の通信回線や搬送波のように、短期にプログラムを保持する「通信媒体」を含むものとする。

【０１６４】

また、「プログラム」とは、任意の言語や記述方法にて記述されたデータ処理方法であり、ソースコードやバイナリコード等の形式を問わない。なお、「プログラム」は必ずしも単一的に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されるものや、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅ

ｍ）に代表される別個のプログラムと協働してその機能を達成するものをも含む。なお、実施の形態に示した各装置において記録媒体を読み取るための具体的な構成、読み取り手順、あるいは、読み取り後のインストール手順等については、周知の構成や手順を用いることができる。

【０１６５】

また、ネットワーク３００は、情報通信端末１００を相互に接続する機能を有し、例えば、インターネットや、イントラネットや、ＬＡＮ（有線／無線の双方を含む）や、ＶＡＮや、パソコン通信網や、公衆電話網（アナログ／デジタルの双方を含む）や、専用回線網（アナログ／デジタルの双方を含む）や、ＣＡＴＶ網や、ＩＭＴ２０００方式、ＧＳＭ方式またはＰＤＣ／ＰＤＣ－Ｐ方式等の携帯回線交換網／携帯パケット交換網や、無線呼出網や、Ｂｌｕｅｔｏｏｔｈ等の局所無線網や、ＰＨＳ網や、ＣＳ、ＢＳまたはＩＳＤＢ等の衛星通信網等のうちいずれかを含んでもよい。すなわち、本システムは、有線・無線を問わず任意のネットワークを介して、各種データを送受信することができる。

【０１６６】

【発明の効果】

以上詳細に説明したように、本発明によれば、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の疎結合情報に分割し、分割された複数の疎結合情報、および、設定された分割ルールを送信するので、送受信される情報の秘匿性を高めることができる情報交換システム、情報通信端末、情報交換方法、プログラム、および、記録媒体を提供することができる。

【０１６７】

また、本発明によれば、複数の疎結合情報、および、分割ルールを受信し、受信した分割ルールに基づいて、複数の疎結合情報から情報を再構成するので、送受信される情報の秘匿性を高めることができる。

【０１６８】

また、本発明によれば、送信手段は、複数の疎結合情報を複数の伝送経路を用

いて送信するので、機密結合度が下げられて生成された複数の疎結合情報をそれぞれ別の通信路を用いて情報交換することができる。また、疎結合情報の対応関係を隠蔽し、送受信される情報の秘匿性をさらに高めることができる。

【０１６９】

また、本発明によれば、要素の名称を別の名称とするためのネーミングルールを設定し、設定されたネーミングルールに基づいて、情報の要素の名称を別の名称にし、設定されたネーミングルールを送信するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【０１７０】

また、本発明によれば、ネーミングルールを受信し、受信した上記ネーミングルールに基づいて、別名化された情報の要素の名称を元の名称に変換するので、オリジナルの情報から別の名称と構造を持つ情報を生成することにより情報漏洩時にオリジナル情報の推定を困難にすることができ、送受信される情報の秘匿性をさらに高めることができる。

【０１７１】

また、本発明によれば、情報は、ＸＭＬにより記載されているので、ＸＭＬデータの分解・再構成の容易性を活かしてＸＭＬデータの機密結合度を下げ、秘匿性を高めることができる。

【０１７２】

また、本発明によれば、ＤＴＤに定義されている要素について、要素の名称、内容および属性のうち少なくとも一つに基づいて機密結合度を設定するので、ＤＴＤに定義されたＸＭＬ情報の要素の内容に基づいて、効率的に機密結合度を設定できる。

【０１７３】

さらに、本発明によれば、疎結合情報は、受信側の情報端末装置において再結合するための再結合情報を含み、分割ルールは、疎結合情報と再結合情報との対応を特定するための情報を含むので、分割された疎結合情報の再結合を媒介する

ための再結合情報を追加することにより、情報の機密性をさらに高めることができる。

【０１７４】

すなわち、乱数等により生成される再結合情報を疎結合情報に付加することにより、第三者が疎結合情報を見たときに、その内容の推定を困難にすることができる。また、どの再結合情報をどの疎結合情報に付加したかを分割ルールにおいて定義することにより、受信側の情報通信端末では、再結合情報に基づいて元の情報に再構成することができるようになる。

【図面の簡単な説明】

【図１】

本システムの全体構成の一例を示すブロック図である。

【図２】

本システムの概要を示す概念図である。

【図３】

本発明が適用される情報通信端末１００の構成の一例を示すブロック図である。

【図４】

本発明が適用される情報通信端末１００の制御部１０２において実行されるソフトウェア構成の一例を示すブロック図である。

【図５】

情報通信端末１００における情報の流れの概要を説明する概念図である。

【図６】

本システムにおける機密結合度の定義の一例を示す概念図である。

【図７】

本発明の疎結合ＸＭＬデータのマルチルーティングの概要を示す概念図である。

【図８】

本発明の要素名の別名化の概要を示す概念図である。

【図９】

デバイダにより実行される要素名の別名化、および、疎結合ＸＭＬデータの作成の一例を示す概念図である。

【図１０】

設定モジュール１０２ａにおける疎結合ＸＭＬの生成に用いる各種ルールの生成の概要を示す概念図である。

【図１１】

再結合情報を用いて情報の分解および再構成を行う場合の一例を示す概念図である。

【図１２】

カード情報を格納したオリジナルＸＭＬ情報の一例を示す図である。

【図１３】

本実施形態における分解／再構成ルールの一例を示す図である。

【図１４】

本実施の形態の分解／再構成ルールに従って分解された疎結合ＸＭＬデータの一例を示す図である。

【図１５】

本実施の形態において受信側の情報通信端末１００のメモリ上にプールされる情報の一例を示す図である。

【図１６】

本実施の形態において初期状態のバファープールに格納される情報の一例を示す図である。

【図１７】

カード番号の要素が分割された疎結合ＸＭＬデータの一例を示す図である。

【図１８】

バファープール中の該当するカード番号要素に、カード番号「１２３４６７８９７９９」がセットされた図である。

【図１９】

全ての疎結合ＸＭＬデータを受信し、バファープール上の各要素にデータをセットした結果を示す図である。

【符号の説明】

１００　情報通信端末

　　１０２　制御部

　　　　１０２ａ　設定モジュール

　　　　１０２ｂ　実行モジュール

　　　　１０２ｃ　ＸＭＬミドルウェア

　　１０４　通信制御インタフェース部

　　１０６　記憶部

　　１０８　入出力制御インタフェース部

３００　ネットワーク

６０１、９０１　オリジナルＸＭＬ

６０２、６０３、８０１、８０２、９０２、９０３　疎結合ＸＭＬ

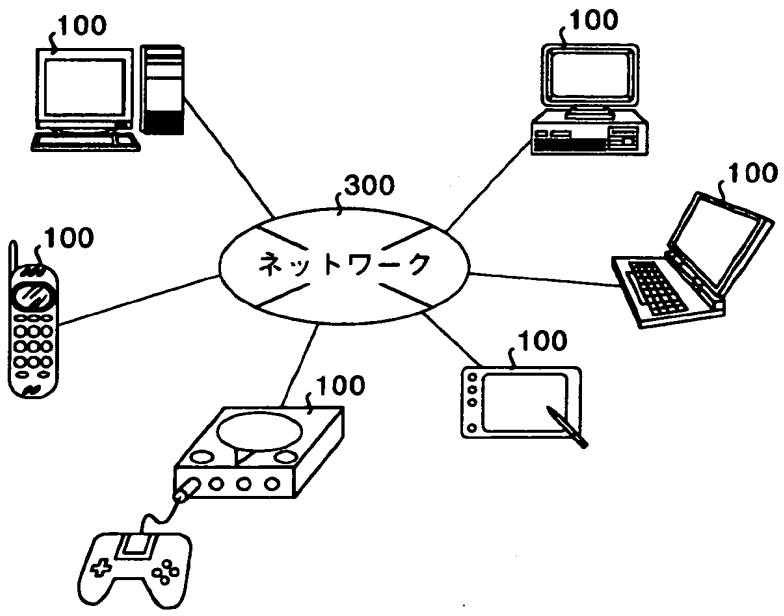
６０４、８０３、１００１、１００２　結合ルール

８０４、８０５　別名ＸＭＬ

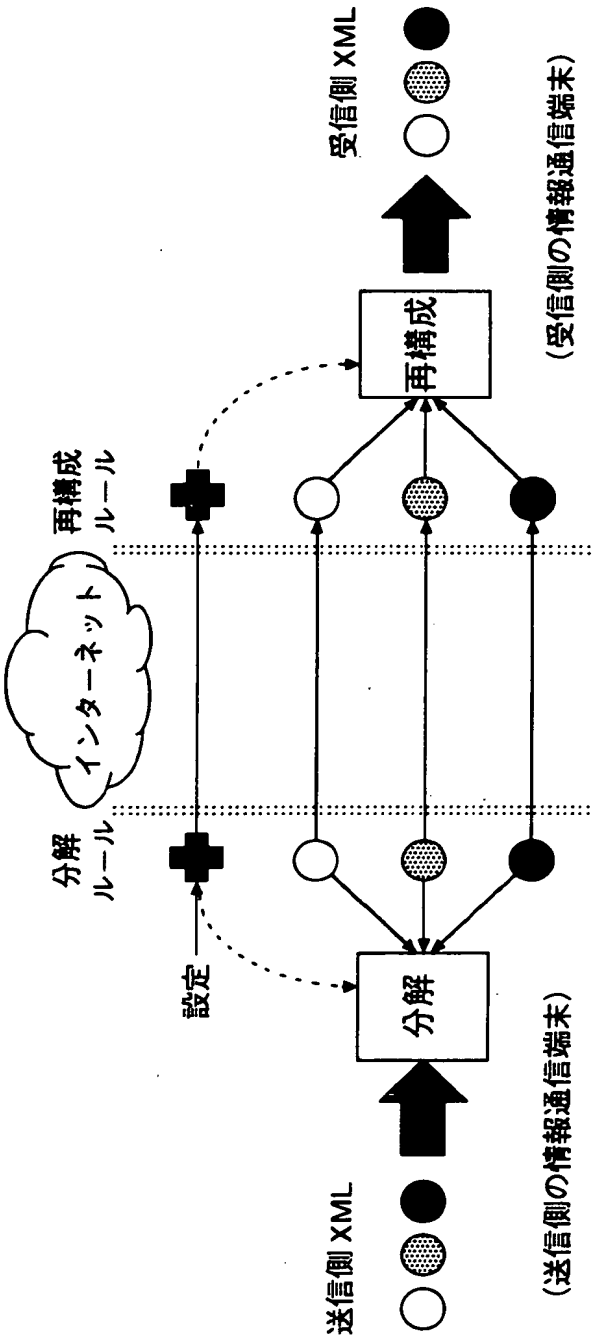
８０６　結合ルールおよびネーミングルール

【書類名】　　図面

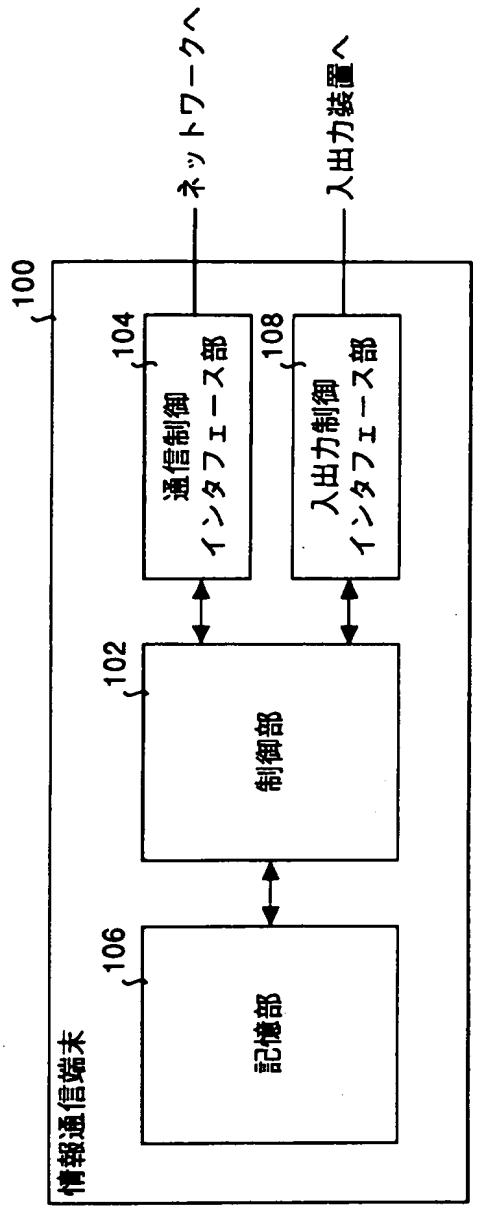
【図１】



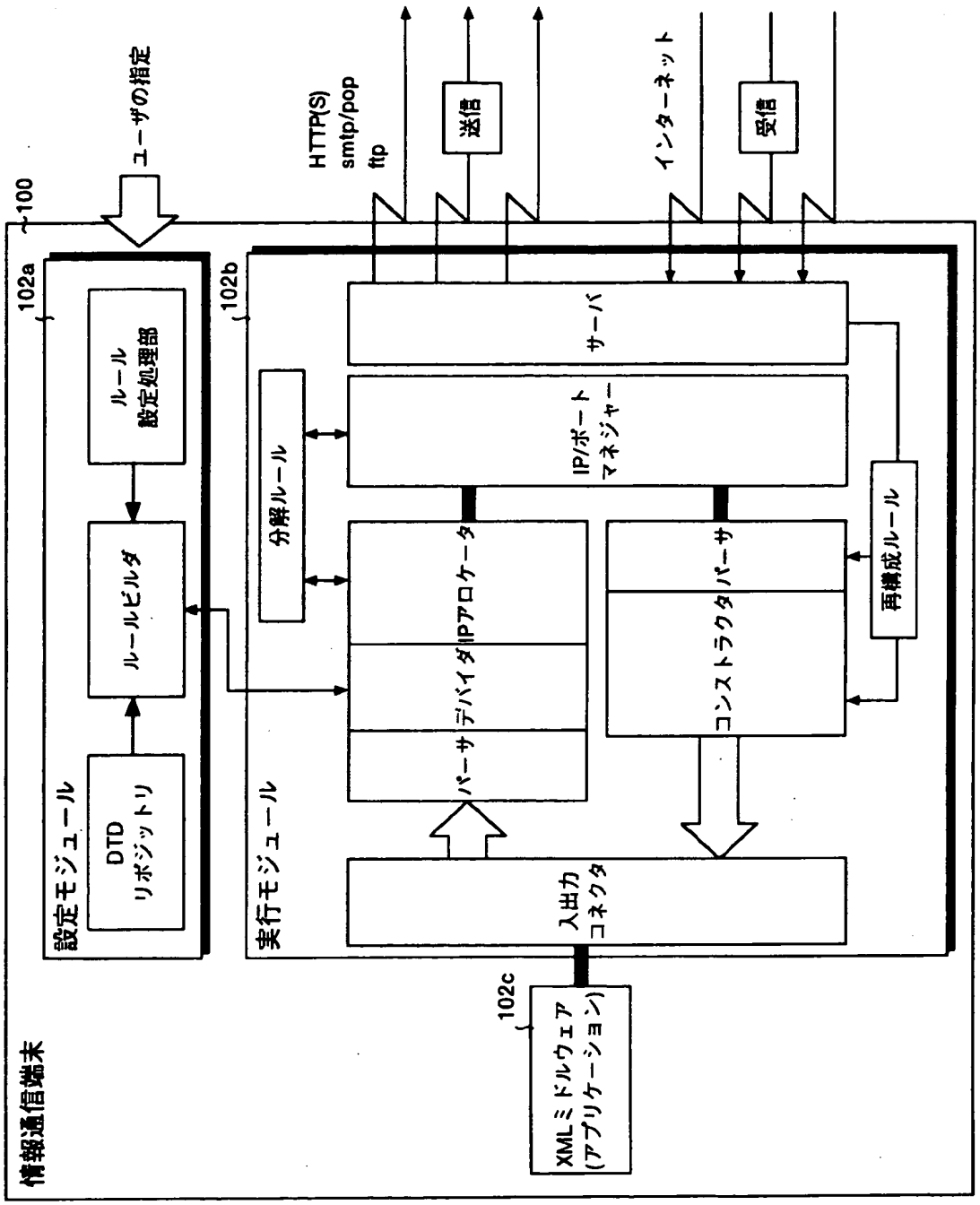
【図２】


受信側 XML
再構成
(受信側の情報通信端末)
再構成
ルール
インターネット
分解
ルール
設定
分解
送信側 XML
(送信側の情報通信端末)

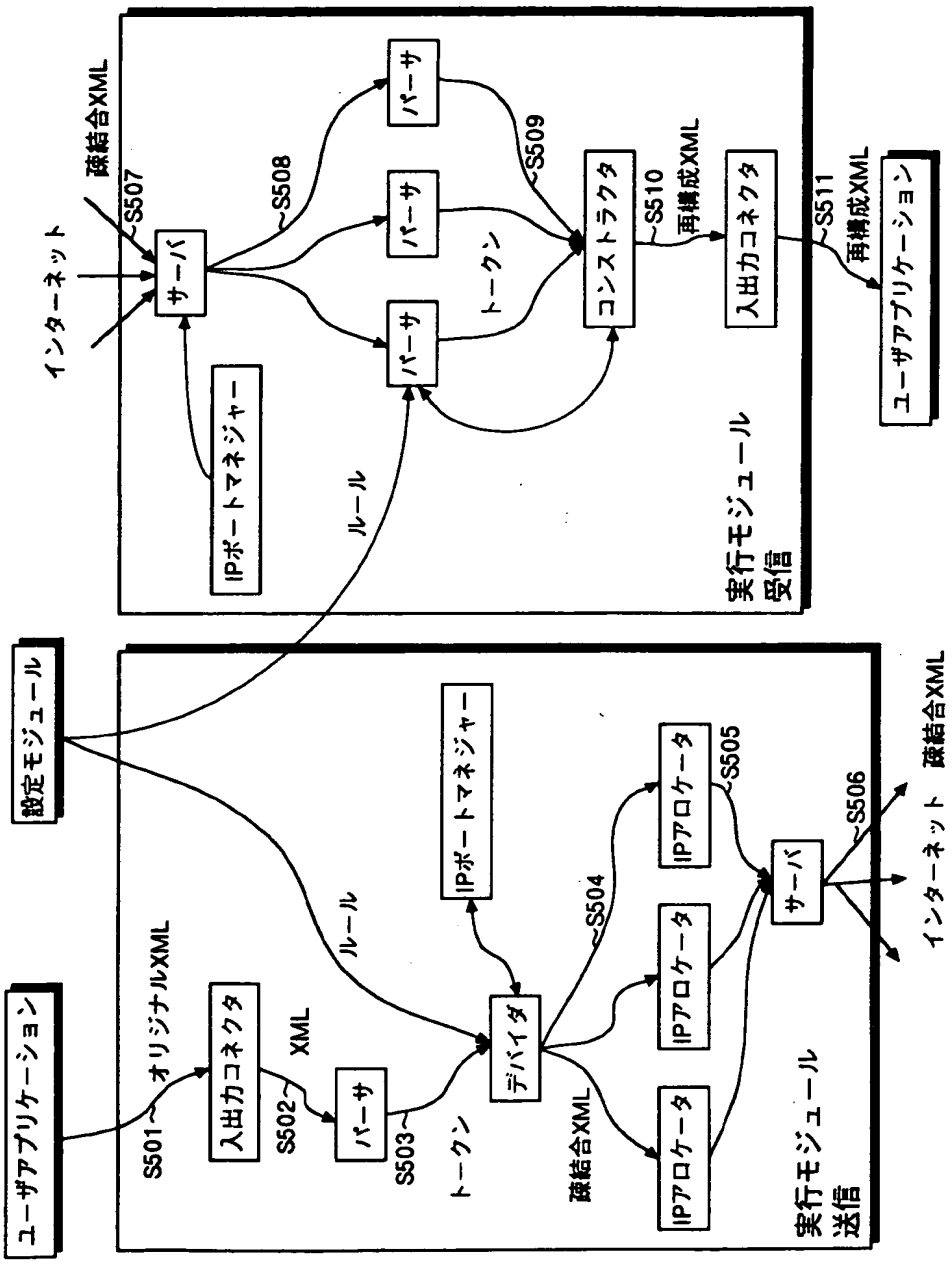
【図３】


ネットワークへ
入出力装置へ
100
104
通信制御
インタフェース部
108
入出力制御
インタフェース部
102
制御部
106
記憶部
情報通信端末

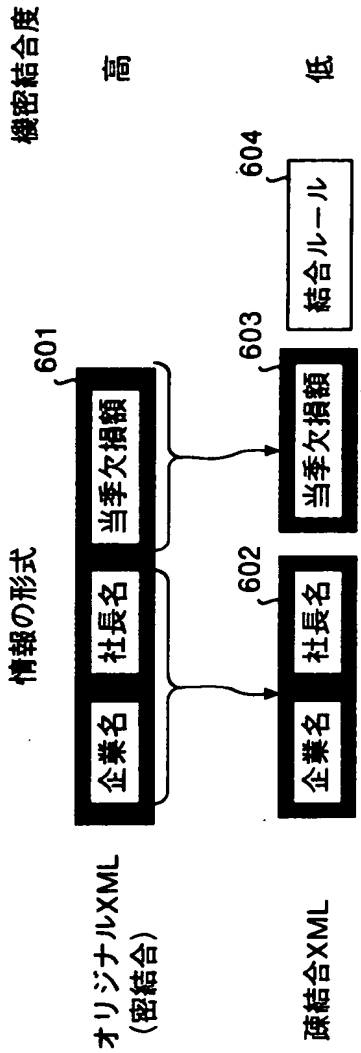
【図４】


情報通信端末
100
ユーザの指定
HTTP(S)
smtp/pop
ftp
送信
インターネット
受信
102a
設定モジュール
ルール
設定処理部
ルールビルダ
DTD
リポジットリ
102b
実行モジュール
サーバ
IP/ポート
マネジャー
分解ルール
パーサ
デバイダ
IPアロケータ
コンストラクタ
パーサ
再構成ルール
入出力
コネクタ
102c
XMLミドルウェア
(アプリケーション)

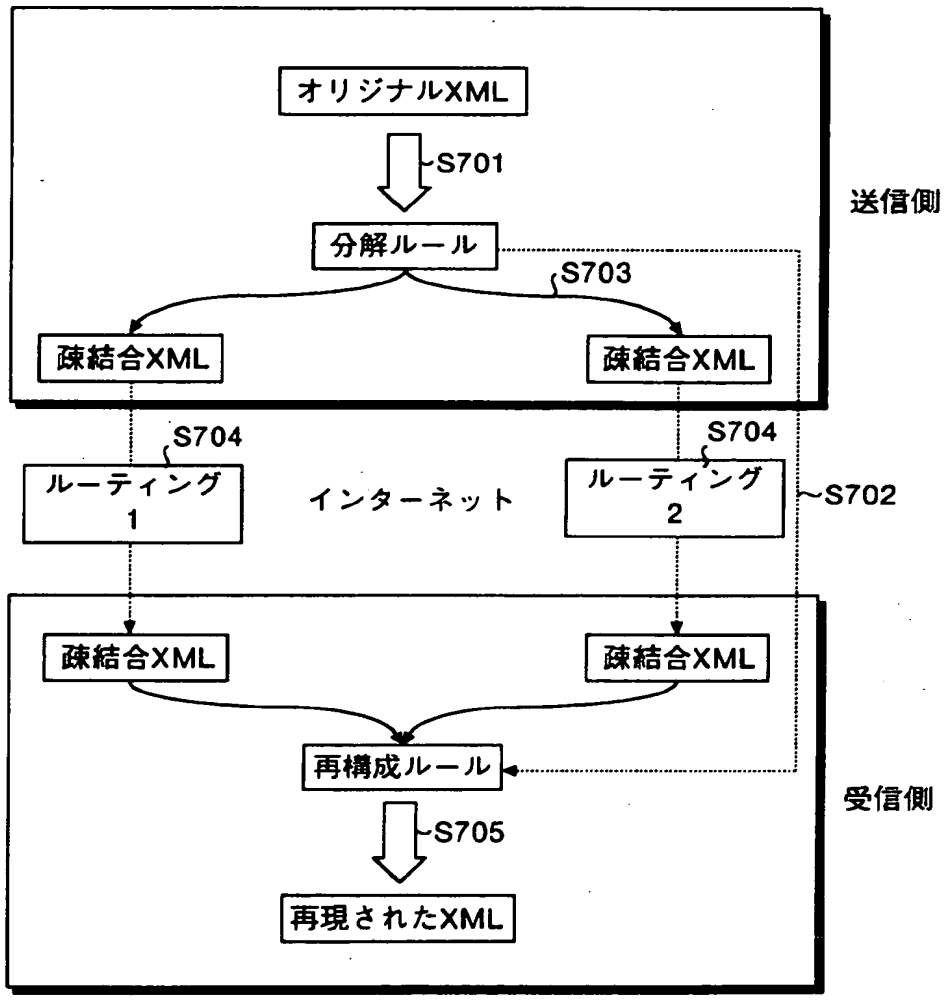
【図５】


ユーザアプリケーション
設定モジュール
S501
オリジナルXML
入出力コネクタ
XML
S502
パーサ
S503
トークン
ルール
IPポートマネジャー
デバイダ
S504
疎結合XML
IPアロケータ
IPアロケータ
IPアロケータ
S505
サーバ
S506
インターネット
疎結合XML
実行モジュール
送信
インターネット
疎結合XML
S507
サーバ
S508
パーサ
パーサ
パーサ
トークン
S509
コンストラクタ
S510
再構成XML
入出力コネクタ
S511
再構成XML
ユーザアプリケーション
IPポートマネジャー
ルール
実行モジュール
受信

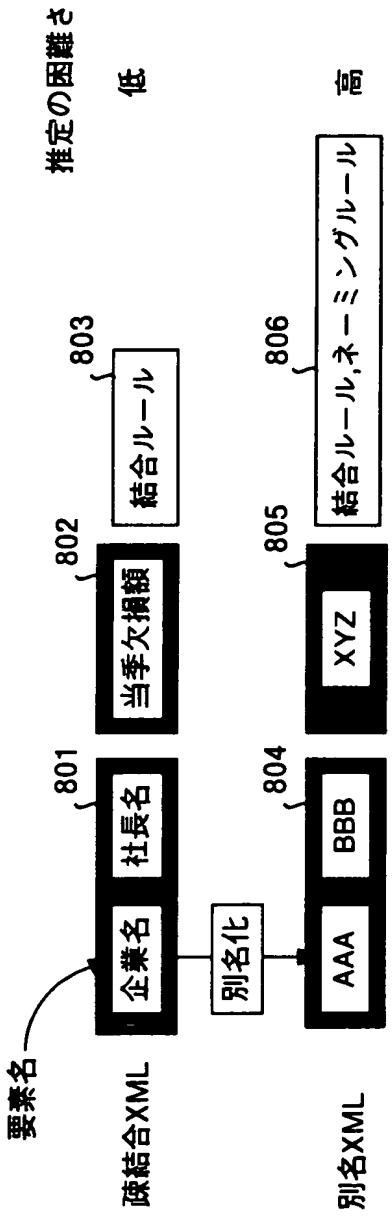
【図６】


機密結合度
高
低
情報の形式
601
603
604
602
企業名
社長名
当季欠損額
当季欠損額
結合ルール
企業名
社長名
オリジナルXML
(密結合)
疎結合XML

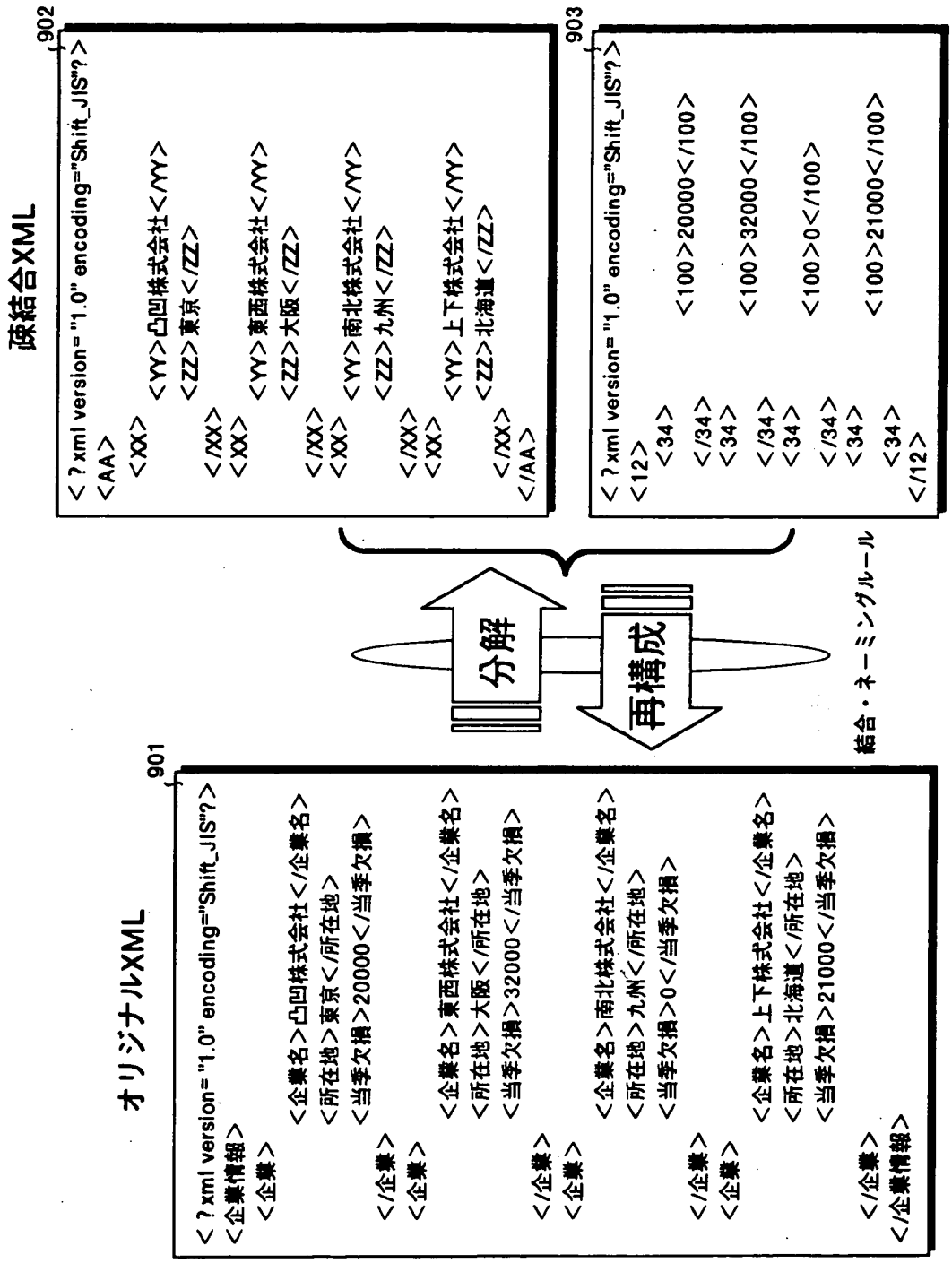
【図７】


オリジナルXML
S701
分解ルール
S703
疎結合XML
疎結合XML
送信側
S704
S704
ルーティング 1
インターネット
ルーティング 2
S702
疎結合XML
疎結合XML
再構成ルール
受信側
S705
再現されたXML

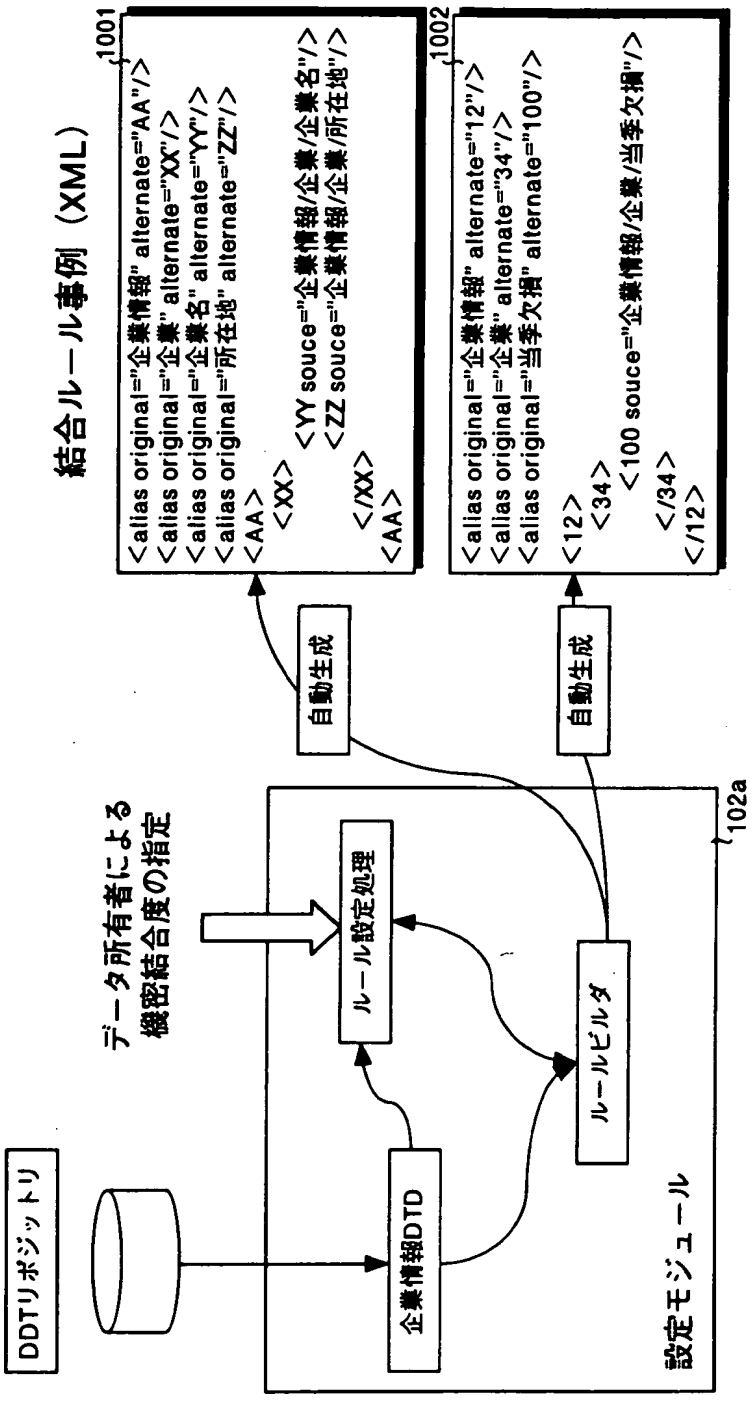
【図８】


推定の困難さ
低
高
803
結合ルール
806
結合ルール,ネーミングルール
802
当季欠損額
805
XYZ
801
社長名
804
BBB
企業名
別名化
AAA
要素名
疎結合XML
別名XML

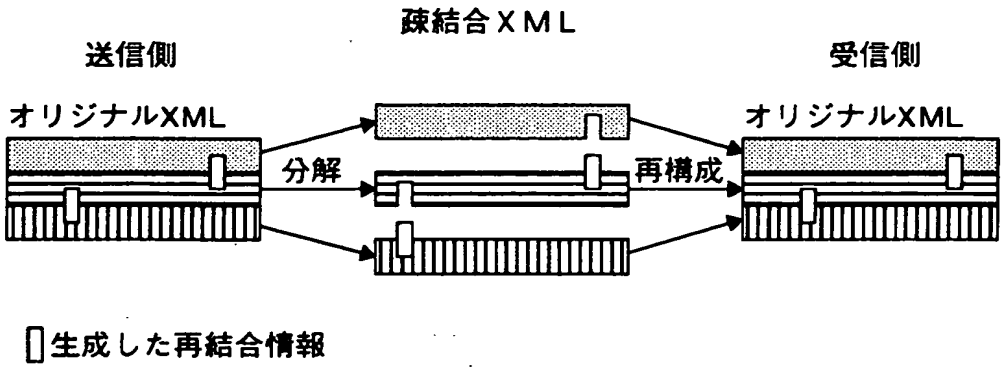
【図９】


疎結合XML
902
<?xml version="1.0" encoding="Shift_JIS"?>
<AA>
<XX>
<YY>凸凹株式会社</YY>
<ZZ>東京</ZZ>
</XX>
<XX>
<YY>東西株式会社</YY>
<ZZ>大阪</ZZ>
</XX>
<XX>
<YY>南北株式会社</YY>
<ZZ>九州</ZZ>
</XX>
<XX>
<YY>上下株式会社</YY>
<ZZ>北海道</ZZ>
</XX>
</AA>
903
<?xml version="1.0" encoding="Shift_JIS"?>
<12>
<34>
<100>20000</100>
</34>
<34>
<100>32000</100>
</34>
<34>
<100>0</100>
</34>
<34>
<100>21000</100>
</34>
</12>
分解
再構成
結合・ネーミングルール
オリジナルXML
901
<?xml version="1.0" encoding="Shift_JIS"?>
<企業情報>
<企業>
<企業名>凸凹株式会社</企業名>
<所在地>東京</所在地>
<当季欠損>20000</当季欠損>
</企業>
<企業>
<企業名>東西株式会社</企業名>
<所在地>大阪</所在地>
<当季欠損>32000</当季欠損>
</企業>
<企業>
<企業名>南北株式会社</企業名>
<所在地>九州</所在地>
<当季欠損>0</当季欠損>
</企業>
<企業>
<企業名>上下株式会社</企業名>
<所在地>北海道</所在地>
<当季欠損>21000</当季欠損>
</企業>
</企業情報>

【図１０】


結合ルール事例（XML）
1001
<alias original="企業情報" alternate="AA"/>
<alias original="企業" alternate="XX"/>
<alias original="企業名" alternate="YY"/>
<alias original="所在地" alternate="ZZ"/>
<AA>
<XX>
<YY souce="企業情報/企業/企業名"/>
<ZZ souce="企業情報/企業/所在地"/>
</XX>
<AA>
1002
<alias original="企業情報" alternate="12"/>
<alias original="企業" alternate="34"/>
<alias original="当季欠損" alternate="100"/>
<12>
<34>
<100 souce="企業情報/企業/当季欠損"/>
</34>
</12>
自動生成
自動生成
データ所有者による
機密結合度の指定
ルール設定処理
ルールビルダ
企業情報DTD
DDTリポジットリ
設定モジュール
102a

【図１１】



出証特２００１－３０７６２２３

【図１２】

オリジナルXMLデータ

```
<my-card>
  <card-no>12346789799</card-no>      ---カード番号
  <password>2345</password>      ----パスワード
  <expiored>2004/01/01</expiored>   ---有効期限
</my-card>
```

【図１３】

分解／再構成ルール

```
<declare variable="@num" binding="abc/zzz:xyz/hed:mix/ifs"/>
<abc>
<xxx source="my-card/card-no"/>
        <zzz source="@num=@random(@timeday)"/>
</abc>
<xyz>
        <123 source="my-card/password"/>
        <hed source="@num"/>
</xyz>
<mix>
        <dsn source="my-card/ expired "/>
        <ifs source="@num"/>
</mix>
```

【図１４】

疎結合XMLデータ

```
‹abc›
  ‹xxx›12346789799‹/xxx›          ---カード番号
  ‹zzz›gj56a02j‹/zzz›          --- 生成した媒介キー
‹/abc›
```

```
‹xyz›
  ‹123›2345‹/123›          ----パスワード
  ‹hed›gj56a02j‹/hed›          --- 媒介キー
‹/xyz›
```

```
‹mix›
   ‹dsn›2004/01/01‹/dsn›       ---有効期限
   ‹ifs›gj56a02j‹/ifs›          --- 媒介キー
‹/mix›
```

【図１５】

```
<buffer>
<binding></binding>      結合の媒介キー
<my-card>
  <card-no></card-no>      ---カード番号
  <password></password>      ----パスワード
  <expired></expired>   ---有効期限
</my-card>
</buffer>
```

【図１６】

バファーの初期状態

```
<buffer>
<binding> </binding>
<my-card>
  <card-no></card-no>      ---カード番号
  <password></password>      ----パスワード
  <expired></expired>   ---有効期限
</my-card>
</buffer>
```

【図１９】

全ての要素にデータをセット

```
‹buffer›
‹binding› gj56a02j ‹/binding›
‹my-card›
  ‹card-no›12346789799‹/card-no›      ---カード番号
  ‹password›2345‹/password›      ----パスワード
  ‹expired›2004/01/01‹/expired›   ---有効期限
‹/my-card›
‹/buffer›
```

【書類名】　　要約書

【要約】

【課題】　比較的手軽な暗号化のような機密保護に加えて、万一それが破られても情報の秘匿性の保持を可能とするものであり、オープンなインターネットを利用しつつ秘匿性が高い情報の交換を安価に実現することのできるシステム等を提供することを課題とする。

【解決手段】　本発明にかかるシステムは、複数の要素を含む情報を送受信する情報通信端末１００がネットワーク３００を介して相互に接続される。送信側の情報通信端末は、複数の要素の機密結合度を設定し、設定された機密結合度に基づいて、情報を複数の疎結合情報に分割するための分割ルールを設定し、設定された分割ルールに基づいて、情報を複数の上記疎結合情報に分割し、分割された複数の疎結合情報および設定された分割ルールを送信する。

【選択図】　　図１

出証特２００１－３０７６２２３

出　願　人　履　歴　情　報

識別番号　　〔５０１１２５９９８〕

１．変更年月日　　２００１年　３月２８日
［変更理由］　新規登録
住　所　　千葉県船橋市習志野台２－２１－４
氏　名　　池田　実

US 0998823703P1

Creation date: 06-02-2004
Indexing Officer: SCHASE1 - SUSAN CHASE
Team: OIPEBackFileIndexing
Dossier: 09988237

Legal Date: 12-19-2001

No.	Doccode	Number of pages
1	IMIS	1

Total number of pages: 1

Remarks:

Order of re-scan issued on .....